UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/740,748	12/19/2003	Tin Qian	224180	4932

45840 7590 10/23/2006

WOLF GREENFIELD (Microsoft Corporation)
C/O WOLF, GREENFIELD & SACKS, P.C.
FEDERAL RESERVE PLAZA
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2112	

DATE MAILED: 10/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/740,748	QIAN ET AL.	
	Examiner	Art Unit	
	Harris C. Wang	2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :12/19/2003, 06/24/2005, 7/22/2005, 4/3/2006.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 5-6, 7-18, 24-31 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Regarding Claims 5-6, data structure does not meet the IEEE definition and is therefore non-functional descriptive material. Non-functional descriptive material per se is an abstract idea and therefore is not statutory, so they are rejected as non-statutory subject material. Also, "computer-readable medium" includes wireless media (pg. 14), which is not statutory. Claims 7-18, 24-31 are rejected for claiming software per se.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Terzis (US 20040243835).

Regarding Claim 1,

Terzis teaches a method for setting firewall policy for an application, comprising: receiving a first parameter comprising information about an application; receiving a second parameter comprising information about a user of the application *("receiving, from the user, a request to access a computer system resource," Claim 1)*;
accessing security level information relating to the first and second parameters; *("determining whether the user is permitted to access at least a portion of a computer system resource based on the user identification information and each of the generated access rules," Claim 1)*

and setting a firewall policy for the application and the user utilizing the security level information. *("distributing each generated access rule to each of the security system sublayers," Claim 1)*

The Examiner determines that when receiving information from a user to request a system resource, information about the application and information about the user must inherently be collected.

Regarding Claim 2,

Terzis teaches the method of claim 1, wherein accessing security level information comprises calling a GetRules method to return rule templates available for the application and user. *("The resource access rules are used to control which users have access to what resources. The resource access rules define priority, source, resource, permission level, allowable identifiers..." Paragraph [0120])*

The Examiner notes that resource access rules are just a subset of several policy rules as shown in figure 6.

Regarding Claim 3,

Terzis teaches the method of claim 1, further comprising, receiving a third parameter regarding trusted contacts, and wherein setting a firewall policy comprises setting the firewall policy for the application and the user and the trusted contacts utilizing the security level information. *("The policy engine may then search the resource access rules...for the user (or User Groups the user belongs to)" Paragraph [0065])*

The Examiner interprets the User Groups as "trusted contacts"

Regarding Claim 4,

Terzis teaches the method of claim 1, wherein setting the firewall policy comprises: setting a default setting for the application; and selecting the default setting for the user. *("generating, based on the access policies, at least one access rule," Claim 1)*

The Examiner interprets at least one access rule as the default setting.

Regarding Claims 5 and 6,

Terzis teaches a computer-readable medium having stored thereon a data structure, the data structure comprising; a first data field representing an application; a second data field representing a user of the application; and a third data field representing available security settings for the user utilizing the application. Where the data structure may also comprise a data object. *("The resource access rules define...source, resource and permission level" Paragraph [0120])*

The Examiner interprets the application as the resource, the user as the source, and the available security settings for the user as the permission level.

Regarding Claim 7,

Terzis teaches an object model for managing a service on a computer, the object model comprising:

a policy object model used to specify one or more policies that the service supports; *("the policy engine talks to the components on the data plane to install and remove filters in response to policy rules," Paragraph [0062])*

and a policy engine platform for interacting with said one or more policies for the service and at least one component that actually performs the service, and to provide said one or more policies to said at least one component. *("The policy interpreter interfaces to the SNMP Agent," Paragraph [0064], Fig 7.)*

The Examiner interprets the policy object model as the "policy engine" and policy engine platform as "policy interpreter."

As seen in Fig. 7, the Policy Interpreter acts as a intermediary between the SNMP agent and the Policy engine. Because the purpose of a SNMP agent is to facilitate information between network components and the purpose of the policy engine is to provide policies, it is inherent that the policy interpreter will provide one or more policies of which one will actually perform the service.

Regarding Claims 8 -10,

Terzis teaches the object model of claim 7, wherein the policy engine platform comprises a rule editor for adding an additional policy in accordance with the policy object model, wherein the rule editor is also configured to delete a policy.

("The interface between the policy engine and the SNMP agent may be used to add and delete policy objects" Paragraph [0064])

The Examiner interprets that editing a policy is the same as adding or deleting a policy.

Regarding Claims 11 and 12,

Terzis teaches the object model of claim 7, wherein the policy engine platform comprises a setting editor configured to automatically generate a policy based upon an application and user combination, wherein the setting editor generates a plurality of policies, and is further configured to permit a user to select from the plurality.

("After a user has successfully logged [in]...the Launch-pad module may contact the policy engine to receive the list of resources that are available to that user...Once fount the policy user may return each of the resources in those rules back to the Launch-pad module, Paragraph [0065])

Where the Launch-pad is defined as a user interface in Paragraph 100. The launch pad screen is capable of displaying "applications...that are specifically made available to that user (Paragraph 106).

Regarding Claim 13,

Terzis teaches the object model of claim 12, wherein the setting editor is further configured to permit setting one of the plurality as a default policy.

("generating, based on the access policies, at least one access rule for each of a plurality of security system sublayers," Claim 1)

The Examiner interprets the at least one access rule as the default policy.

Regarding Claim 14,

Terzis teaches the object model of claim 7, wherein the policy engine platform comprises a rule explorer for providing a view of the one or more policies.

Because the policy interpreter interfaces between the SNMP agent and the policy engine (Fig. 7) it is inherent that there will be a component that allows a view of one or more of the policies.

Regarding Claim 15,

Terzis teaches the object model of claim 7, wherein the policy object model comprises a policyrule object usable to generate policy, the policyrule object comprising a condition property and an action property, wherein a policy generated by the policyrule object is configured to perform an action in the action property responsive to a condition in the condition property being met. (Fig. 6, 670)

Regarding Claim 16 and 24,

Terzis teaches the object model of claim 7, wherein the service is a firewall service. *("According to one embodiment the rules are generated and installed at the firewall level" Paragraph [0019])*

Regarding Claim 17,

Terzis teaches the object model of claim 7, wherein the policy engine platform is configured to deny providing said one or more policies to the component if a requester is not authorized. ("*Based on the policies associated with that user, a set of specific access rules are generated that enable the subsystems to provide filtering and deny access to prohibited resources and services." Paragraph [0088])*

Regarding Claim 18,

Terzis teaches the object model of claim 17, wherein determining whether a requester is authorized comprises comparing a provider rank for the requester against a permitted rank, and if the provider rank for the requestor does not meet or exceed the permitted rank, denying the requester. (Fig 6. 675, PermissionLevel)

The Examiner interprets the parameter PermissionLevel under the Resource Access Rules as rank. Where the PermissionLevel is checked against a permitted PermissionLevel and if the PermissionLevel does not meet or exceed the permitted rank, to deny the requestor.

Regarding Claim 19,

Terzis teaches a method of managing a service on a computer, the method comprising: specifying, via a policy object model, one or more policies that the service supports; *("The policy engine talks to the components on the data plane to install and remove filters in response to policy rules," Paragraph [0062])*

and interacting, via a policy engine platform, with said one or more policies for the service and at least one component that actually performs the service; *("the Launch-pad module may contact the policy engine to receive the list of resources that are available" Paragraph [0065])*

and providing, via the policy engine platform, said one or more policies to said at least one component. *("Once found the policy engine may return each of the resources in those rules back to the Launch-pad module" Paragraph [0065])*

Regarding Claim 20,

Terzis teaches the method of claim 19, further comprising automatically generating a policy based upon an application and user combination. *"After a user has successfully logged into the MACSS, the Launch-pad module may contact the policy engine to receive the list of resources that are available to that user," Paragraph [0065])*

Regarding Claim 21,

Terzis teaches the method of claim 20, further comprising generates a plurality of policies, and permitting a user to select from the plurality. *("Once found the policy engine may return each of the resources in those rules back to the Launch-pad module" Paragraph [0065])*

As described before the Launch-pad module is a user interface. Examples can be found in Fig. 4 and Fig. 5.

Regarding Claim 22,

Terzis teaches the method of claim 21, further comprising setting one of the plurality as a default policy. *("generating, based on the access policies, at least one access rule for each of a plurality of security system sublayers," Claim 1)*

The Examiner interprets the at least one access rule as the default policy.

Regarding Claim 23,

Terzis teaches the method of claim 22, further comprising authorizing a user prior to providing. *("the Launch-pad module may contact the policy engine to receive the list of resources that are available" Paragraph [0065])*

Regarding Claim 25,

Terzis teaches the object model of claim 24, further comprising an IPSecRule derived from the policyrule object, the IPSecRule being configured to trigger an IPSec callout when an IPSec condition is matched, and to indicate configuration parameters for securing traffic related to the callout. (Fig. 14, 1440).

The services dispatcher connects to the launch-pad which connects to the policy engine.

Regarding Claim 26,

Terzis teaches the object model of claim 25, wherein the IPSecRule evaluates a standard 5-tuple to determine if a condition has been met. (Fig. 11)

Regarding Claim 27,

The object model of claim 24, further comprising a KeyingModuleRule derived from the policyrule object, the KeyingModuleRule being configured to select which key negotiation module to use when there is no existing secure channel to a remote peer.

("The key exchange field specifies how keys are exchanged and determines what key parameters will be used." Paragraph [0130])

The Examiner interprets key negotiation as key exchange. The Examiner notes that the key exchange field is part of the security rules, which is part of the policy rules.

Regarding Claim 28,

Terzis teaches the object model of claim 27, wherein the KeyingModuleRule evaluates a standard 5-tuple to determine if a condition has been met. (Fig. 11)

Regarding Claim 29,

Terzis teaches the object model of claim 24, further comprising a IKERule derived from the policyrule object and configured to specify the parameters for carrying out Internet Key Exchange key negotiation protocol. (Fig. 14, IKE)

Regarding Claim 30,

Terzis teaches the object model of claim 29, wherein the IKERule evaluates a local address and a remote address to determine if a condition has been met. This step is inherent in IKE protocol.

Regarding Claim 31,

Terzis teaches the object model of claim 29, wherein the IKERule comprises an IKEAction action property that defines the authentication methods for performing Internet Key Exchange key negotiation protocol. *("The key exchange field specifies how keys are exchanged and determines what key parameters will be used." Paragraph [0130])*

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 7:30-5, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 5712721497. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

Walter D. Griffin

WALTER D. GRIFFIN
SUPERVISORY PATENT EXAMINER